Centrum für Europäische Politik
FREIBURG | BERLIN

cepAdhoc

No. 17 | 2024 9 August 2024

Drones are Stressing the Security Services

Modern aerial devices are placing high demands on defence capabilities

Anselm Küsters and Jörg Köpke

© shutterstock/ Dmitry Kalinovsky

Whether in agriculture, film production or parcel delivery: drones have become an integral part of modern life. But as they become more widespread, the risk of misuse, such as for crime or terrorism, increases. The threat of drone attacks is still underestimated and needs to be combated with sophisticated defence systems that are not yet available.

- More than 90 per cent of the drones currently in use are controlled by radio, but the number of drones that operate via mobile networks such as LTE/5G or autonomously is increasing. This could reveal gaps in capability if existing defence systems are not designed to deal with this technology.
- In addition, major events, such as the European Football Championships in Germany or the Olympic Games in Paris, are putting even greater pressure on security services to develop effective defence measures. During the European Football Championships, unauthorised drone flights were detected at all venues in Germany although it was a criminal offence to fly within the prohibited zone of a tournament city.
- In addition to the military aspects, civilian applications, such as pop concerts, water management and data centres, also need to be taken into account. Drone defence should become part of regular perimeter protection, for example as part of the KRITIS umbrella act. In addition, the planned partnership between the European Investment Bank and the NATO Innovation Fund must be significantly expanded in financial terms.

Table of contents

1 Introduction: Underestimating the danger from above

Drones have become an integral part of modern life in many sectors. They are used in agriculture, film production and parcel delivery. However, as they become more widespread, the risk of misuse, such as for criminal activities or terrorist attacks, is also growing. Drones can transport explosives or perform surveillance tasks, as was the case with the overflights of French nuclear facilities a few years ago[1], or most recently in the forests outside Berlin, when drones of unknown but presumably Russian origin observed the training of Ukrainian soldiers.[2] The threat posed by drone overflights and drone attacks is often underestimated by authorities and representatives of the private sector in Germany and needs to be taken more seriously.

This is due not least to major technological changes that have occurred in recent years, triggered by the Russian war of aggression against Ukraine, and continued more recently in the Nagorno-Karabakh conflict, in which Azerbaijan successfully deployed Israeli Harop combat drones.[3] Over 90 per cent of drones in use today are controlled by radio, but the number of drones operating via mobile networks such as LTE/5G is increasing. **According to experts, this gives rise to serious capability gaps in defence as existing defence systems are often not designed to deal with this technology.** The recent use of an Iranian Samad-3 drone in the Houthi attack on Tel Aviv, which, with slight modifications, was presumably able to evade Israeli reconnaissance systems and head for targets 2,000 to 3,000 kilometres away,[4] also underlines the urgency for Europe to build up its arms in this area. On 14 July, the Federal Public Prosecutor's Office arrested a member of Hezbollah who was intending to procure components in Germany, most notably engines, for the construction of military drones for terrorist attacks against Israel.[5]

In addition, major events, such as the European Football Championship in Germany and the Olympic Games in Paris, have put even greater pressure on security services to develop effective defence measures. During the European Football Championship, unauthorised drone flights were detected at all venues. Nationwide figures are not available but, according to a dpa survey, there were 86 police operations due to drones near stadiums during European Championship matches in North Rhine-Westphalia alone.[6] In Stuttgart, several drones violating the no-fly zone were intercepted early.[7] Industry experts estimate that this is just the tip of the iceberg. The figure for all the venues combined must have been in the thousands, although it was a criminal offence to fly within the prohibited zone of a tournament city. Not only did they jeopardise the safety of the event but also strained the nerves of the people in charge because intelligence services feared IS attacks with "suicide drones".[8] There were no drone attacks during the European Championships and, according to the police, pilots mainly broke the law unintentionally, but it was not just amateurs involved.

---

1 Lessat (2024), Angriff aus heiterem Himmel - Ausgabe 194 (kontextwochenzeitung.de).
2 Bewarder und Flade (2024), Fast 450 Drohnen über Bundeswehrstandorten gesichtet | tagesschau.de.
3 Goertz (2021), Krieg um Bergkarabach Drohnen können Kriege entscheiden.pdf (asmz.ch).
4 Hoffer (2024), Was der Huthi-Drohnenangriff auf Tel Aviv für Israel bedeutet (nzz.ch).
5 See: Der Generalbundesanwalt - Festnahme eines mutmaßlichen Mitglieds der ausländischen terroristischen Vereinigung „Hizb Allah“ („Hisbollah“).
6 WDR (2024), 86 Polizeieinsätze wegen Drohnen an EM-Stadien in NRW - Fußball - Sport - WDR.
7 Klass und Rudat (2024), Seit EURO 2024-Start schon fünf Drohnen in Stuttgart abgefangen - SWR Aktuell.
8 Daniel (2024), Geheimdienste fürchten IS-Anschläge mit Drohnen während Euro - Politik-Live (oe24.at).

2 Defence: Detecting drones

Drone flights are clearly regulated in Germany and Europe. In line with the federal structure of the Federal Republic of Germany, the aviation authorities of the federal states are responsible for all administrative acts in connection with the take-off and operation of drones used for civilian purposes. Local safety authorities deal with aerial craft at lower altitudes. In Germany, drones, or unmanned aerial vehicles (UAVs), are allowed to fly at a maximum height of 120 metres.

Drones are usually detected by the security authorities using a combination of different technologies such as radar, radio, acoustics and camera sensors. Audio sensors, for example, can detect noises within a radius of a few hundred metres, while video sensors that analyse movement patterns require a line of sight to the drone. Purely manual audio or video-based detection is therefore often too slow. The use of artificial intelligence (AI) makes it possible to analyse the resulting patterns and sounds more efficiently based on the data obtained from the sensors. A geopositioning process, involving multiple consecutive observations of the same drone, enables continuous tracking of the drone.[9] Algorithms compare the recognised signals with a library of known drone transmissions and identify the drone activities. This also allows the drone operator's location to be precisely identified so that the person can be approached covertly or overtly by the security authorities.

Detecting potentially dangerous drones has become a critical issue for security authorities. According to German air traffic control, the majority of existing detection systems, most of which originate from military applications, often prove to be inefficient and unreliable. Tests at Frankfurt and Munich airports in 2020 showed that many of the existing systems fail due to different topographies or the need to distinguish drones from other objects. One key finding is that there is no universal solution. At the same time, key decision-makers have recognised and described the basic requirements that a drone detection system must meet. The English-language study on these tests, which is still widely cited in specialist circles today, states that the requirements for current detection systems arising from new drones were met "to different degrees, but in no case sufficient", which leads the authors to conclude: "Airports seem to be a very challenging environment for DDS [Drone Detection Systems], and we think that yet a lot of development has to be undertaken to combine the best components from different brands to establish a workable solution".[10] In the first half of this year, 75 incidents involving drones were reported in German airspace, a slight increase on the previous year.[11]

During the 2024 European Football Championships in Germany, drone defence initially consisted of a technically monitored flight ban within a certain radius of the stadiums. According to press reports, the Deutsche Telekom subsidiary T-Systems received an order worth more than two million euros from the Berlin police to protect the city from drones during the European Championships. This included a system using sensors to analyse the radio spectrum and locate drones and their pilots[12], with the focus on detection rather than defence. The latter was provided by the police who were on site in all European Championship cities with electronic equipment, including shoulder-mounted jammers like those used by the German armed forces.[13] These devices can interrupt the connection between the

---

9 Lehmann (2024), Drohnenabwehr im Zuge der Uefa Euro 2024 | Protector.

10 Heidger, Lambercy und Lambers (2021), "Tracking Analysis of Drone Detection Systems at Airports: Methodology and Results," 2021 21st International Radar Symposium (IRS), Berlin, Germany, p. 15.

11 DPA (2024), Deutscher Luftraum: Drohnen behindern Flugverkehr – 75 Vorfälle im ersten Halbjahr 2024 - DER SPIEGEL.

12 Heuzeroth (2023), Telekom soll Fußball-EM in Deutschland vor Drohnen schützen - WELT.

13 Kalus (2024), Reul: Drohnen-Abwehr bei der Fußball-EM ist startklar - Nachrichten - WDR.

drone and the ground control station and stop the drone, force it to land or send it back to the starting point in order to identify the pilot. When a drone was detected, specialists could check whether it was dangerous and, in case of doubt, bring it down in a controlled manner .

However, urban environments, which are the usual venue for major sporting and cultural events, pose a particular challenge for drone defence. High building density, legal restrictions and a large number of radio transmitters make monitoring difficult. To ensure the most comprehensive coverage possible, sensors must be placed strategically to avoid so-called dead zones, i.e. areas with limited or no detection.[14] The usual distance between sensors is two to four kilometres in urban areas and three to six kilometres in rural areas. Civilian, police or military **radio masts are suitable places to locate passive sensors for detecting drones.** This method offers the advantage of earlier warning compared to radar and video sensors, which often only allow for short response times. Companies such as Deutsche Telekom therefore favour the use of this infrastructure. Other providers of drone detection and defence are ESG, part of the Hensoldt Group, as well as the internationally active family business Rohde & Schwarz and the Dutch specialist Robin Radar. Regardless of the type of sensor, the speed of the response time from detection to contact with the pilot by security forces or interception of the drone, remains a challenge. The seamless integration of detection systems into the command and control systems of security authorities via interfaces is therefore the next logical step.

A broader view of drone defence is therefore urgently needed. In addition to military aspects**, civilian applications also need to be taken into account, such as major events,** water management and data centres. Drone defence should become part of regular perimeter protection, so that protection by means of video, fencing and access control would be extended to include the dimension of air security. Small detection systems can detect drone overflights in the area or in sections of the property. The detection systems record and document drones and their remote control systems and enable a clear visualisation of all events.

According to experts, a combination of detection and defence is also appropriate for critical infrastructure.[15] Detection measures alone are often not enough and require the addition of defence technologies which can intercept the drone or render it harmless in a controlled manner. These measures can be flexibly integrated into existing structures or operated autonomously with just a notification of any detection alerts and defence measures undertaken. The protection of critical infrastructure is being expedited by the planned KRITIS umbrella act, which sets out clear rules and binding security measures. According to the Federal Office for Information Security, there are more than 1,000 KRITIS operators in Germany with a total of around 2,000 systems in the eight sectors of energy, water, food, IT and telecommunications, health, finance and insurance, transport and traffic, and waste disposal. The new law, which is due to come into force in October, requires operators of such infrastructure to comprehensively analyse the threat situation and implement measures to protect against drone attacks.

For these KRITIS operators, drone tracking technology must be energy-efficient, must not cause interference with other electromagnetic technologies and should be able to recognise autonomous drones that do not emit their own signals.[16] A team from Fraunhofer FKIE has investigated the use of the new 450 megahertz mobile phone network and demonstrated in tests that passive radar based on

[14] Lehmann (2024), Drohnenabwehr im Zuge der Uefa Euro 2024 | Protector.
[15] Kupferer (2023), Wie Kritis-Betreiber Drohnen effektiv abwehren | Protector.
[16] See on this: Klein (2024), Blackout und Drohnen: Wie Kritis-Betreiber sich auf neue Gefahren einstellen - Table.Media.

these signals is suitable for tracking drones. However, critics warn that the unclear positioning of pylons and inadequate protection of underground cables could lead to operators of critical infrastructure being lulled into a false sense of security and vulnerabilities could arise in the event of a failure.[17] Thus, there does not yet appear to be a comprehensive solution.

3 Attack: Drones in war

In addition to these enhanced defence strategies, the current geopolitical situation also requires more technological innovation in Europe to compensate for the defensive capability gap. Russia's invasion of Ukraine has taken the drone war to a new level. Inexpensive but effective first-person view attack drones controlled via a virtual reality headset have at least temporarily alleviated some of the Ukrainian army's artillery problems. Ukraine has the capacity to produce 150,000 drones per month and could produce a total of two million by the end of the year.[18] More than 200 Ukrainian companies are working on drone projects, just under 60 of which have been awarded government contracts. To evade Russian attacks, volunteers are using online resources to manufacture drones in inconspicuous workshops.[19] With the help of AI-controlled software, these drones can home in on Russian targets and are more resistant to electronic jamming attempts, as the Centre for European Policy described back in May 2023.[20] Ukraine's drones, whose range extends into Russian territory, have long since become recognised as "high-tech weapons"[21].

The rapid development and miniaturisation of drone technologies and their direct use on the battlefield therefore represents a major challenge for Europe's defence capabilities. The war over Nagorno-Karabakh demonstrated the military effectiveness of combat drones and the fatal consequences of a lack of drone defence. Since then, both the procurement of defence systems and the introduction of reconnaissance and combat drones have become matters of urgency for the German army in order for it to hold its own against well-equipped opponents in an emergency.[22] Still, conventional weapons programmes take years, sometimes decades, to develop and rely on substantial government budgets and large research and testing facilities. Drones, on the other hand, are not only cheap and quick to produce but also more versatile and harder to detect. New AI-controlled drones can also make autonomous decisions and adapt their tactics in real time, which increases their unpredictability. In future, drones will be able to operate autonomously and in swarms, which also means they could be used for both military and civilian purposes, such as searching for missing persons.[23] Thus, state and non-state actors will then be able to effectively circumvent conventional defence mechanisms by deploying swarms of drones.

From a technical point of view, it will be extremely difficult to defend against the drone swarms of the future. The enormous bandwidth of the signals used means that it is difficult to block all the frequencies that can be used to control drones. Drones can operate on a variety of frequencies, which can be constantly changed or modified to avoid jamming attempts. According to experts, the use of

---

17 See on this: Klein (2024), Blackout und Drohnen: Wie Kritis-Betreiber sich auf neue Gefahren einstellen - Table.Media.

18 Court (2024), Deputy minister: Ukraine can produce 150,000 drones per month (kyivindependent.com).

19 GlobalData (2024), Ukraine's drone production ramps up - Airforce Technology (airforce-technology.com).

20 Küsters und Köpke (2023), Vorteil Ukraine: Wie KI die Kräfteverhältnisse im Krieg verändert (cepAdhoc) | cep - Centrum für europäische Politik.

21 Eigendorf (2024), Krieg in der Ukraine: Hightech und KI als Hoffnung - ZDFheute.

22 Gady (2021), Krieg um Berg-Karabach 2020: Implikationen für Streitkräftestruktur und Fähigkeiten der Bundeswehr | Bundesakademie für Sicherheitspolitik.

23 FAZ of 10 July 2024, "Drohnenschwärme für Deutschlands Sicherheit".

geofencing jamming technology would also paralyse communications systems over a large area and thereby also affect our own troops, as these systems operate on the same or neighbouring frequencies.[24]

This upheaval is now also disrupting the defence industry. The rapid spread of drones on the battlefield is shaking up the established hierarchy of global defence companies, as the *Financial Times* recently revealed in a detailed report.[25] New players, such as AeroVironment, known for its Switchblade drone, and technology start-ups such as Palantir Technologies, Rebellion Defense and the European AI specialist Helsing, are challenging established companies such as Lockheed Martin, Raytheon and BAE Systems, which have dominated the defence sector for decades. These traditional defence companies frequently respond to the growing competition and industrial challenges with partnerships or takeovers. One example of this is Saab, which acquired a five per cent stake in Helsing last year in order to assimilate its AI-based software solutions. Experts also believe that quantum computers are on the verge of practical application, with American companies once again leading the way and Germany having to find its own niche; Germany's Cyberagentur has therefore commissioned research into mobile quantum computers that are intended to provide high computing power in crisis areas.[26]

4 What can be done?

In order for these partnerships to result in sufficiently rapid protection for European countries, more long-term public investment is needed. With that in mind, NATO member states set up an innovation fund worth one billion euros in July of this year to promote start-ups and companies in the defence sector.[27] The aim of this initiative is to strengthen the European defence industry and increase innovation in the areas of security and resilience. In view of the current threat situation and technological challenges, this step is necessary and overdue.

The partnership between the European Investment Fund (EIF) and the NATO Innovation Fund (NIF), sealed by a Memorandum of Understanding signed in Brussels, promises closer cooperation and more financial support for start-ups and SMEs. Specifically, the EIF, part of the European Investment Bank Group (EIB), and the NIF, an independent venture capital fund supported by 24 NATO countries, want to pool their resources to create an ecosystem for sustainable growth. The collaboration is also aiming to channel more private capital into security-relevant technology areas.

However, despite these positive developments, the question remains as to whether one billion euros is really enough to meet the challenges of modern defence and security. In light of the aforementioned developments in the deep tech industry, such as the combination of mobile quantum computing and drone swarms, the financing requirements could be significantly higher. A look at the international picture shows that other major powers such as the USA and China are investing significantly more in their defence technologies. The growing role of AI in American and Chinese military projects[28] and the threat from cyber-attacks also indicates a need for massive and

[24] Posaner und Gonzalez (2024), POLITICO.
[25] FT (2024), The age of drone warfare is disrupting the defence industry (ft.com).
[26] See comments by Christian Hummert in the German newspaper FAZ of 10 July 2024, "Drohnenschwärme für Deutschlands Sicherheit".
[27] EIB (2024), EIF and NATO Innovation Fund join forces to unlock private capital for Europe's defence and security future (eib.org).
[28] Bresnick (2024), China's Military AI Roadblocks | Center for Security and Emerging Technology (georgetown.edu).

long-term investment in research and development on the European side in order to remain at the forefront. This paradigm shift has yet to become a reality.

The increasing willingness of investors to invest in companies in the defence industry also implicitly bears out the new trend. According to investors, while large funds that invest exclusively in dual-use technologies or armaments are already being set up in the USA, Europe is lagging behind.[29] A **more flexible and better coordinated procurement policy in Europe** would be helpful here and could be organised by an EU Commissioner for Defence, after the new Commission takes office. The Commissioner could act as mediator for the Member States who still have important legal competences in this area. Dual-use companies, which produce for both civilian and military applications, play a key role here. This also provides another strong argument in favour of a better capital markets union in Europe, which would promote private investment in order to overcome public financing bottlenecks. Not only would this benefit the defence industry, but also Europe's technological innovative strength as a whole.

5 Conclusion

The European Football Championships in Germany and the Olympic Games in France are prime examples highlighting the existing capability gap in drone defence. It is essential to consider both the military and civilian aspects of drone defence, especially with regard to critical infrastructure. History shows that technological advancements, such as the tank in the World War I and the atomic bomb in World War II, were decisive turning points in warfare. In the wars of the present day and the future, drones may be the next in line to be accorded such significance.

[29] Friederichs (2023), Project A: "Es gibt ein großes Interesse von Investoren am Militär" | ZEIT ONLINE.

Authors:

Dr Anselm Küsters, Head of Digitalisation & New Technologies
kuesters@cep.eu

Dr Jörg Köpke, Head of Communications at the Centrum für Europäische Politik
koepke@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin
Tel. + 49 761 38693-0

The **Centrum für Europäische Politik** FREIBURG | BERLIN, the **Centre de Politique Européenne** PARIS and the **Centro Politiche Europee** ROMA form the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

The Centres for European Policy Network analyses and assesses the policy of the European Union independently of individual or political interests, in alignment with the policy of integration and according to the principles of a free, market-based system.