Drones and Counter-Drone Technologies: Understanding Their Legality in Cyprus

By Michael Ioannou, Chief Information Officer, and Emilios Charalambous, Associate at Elias Neocleous & Co. LLC.

The rapid proliferation of drones across Europe has reshaped entire sectors from commercial photography and media production to infrastructure inspection, public safety operations, and environmental monitoring. Cyprus is no exception to this trend. As unmanned aerial vehicles (UAVs) become increasingly accessible and capable, the parallel growth of public concern over privacy, safety, and the potential misuse of drones has fuelled heightened interest in so-called “anti-drone” or counter-UAV technologies.

Yet, while the market for such systems is expanding rapidly, the legal framework governing their use is significantly more restrictive than many stakeholders appreciate. A common misconception is that the technology’s availability on the international market implies that its deployment is lawful. In reality, Cyprus consistency with the broader EU legal landscape maintains **strict limits** on both drone operations and the use of equipment intended to detect, disrupt, or intercept them.

Understanding these limits is essential for businesses, municipalities, private security firms, and individuals considering the acquisition or use of counter-drone solutions.

Drone Operations: Regulated, Not Prohibited

Drone operations in Cyprus are governed primarily by Regulation (EU) 2019/947 on drone operations and Regulation (EU) 2019/945 on drone product standards. Together, these instruments establish a harmonized regulatory environment for drone flights across the EU.

Under this framework, most drone operators are required to register, complete minimum training, and comply with flight restrictions, including those related to height, proximity to people, and designated no-fly areas. The Cypriot Department of Civil Aviation (DCA) enforces these rules and frequently issues local directives to ensure safe operation within national airspace, with the Civil Aviation Decisions of 2015, (i) 403/2015 and (ii) 402/2015, leading the way as they developed the conditions for operation and exceptions.Perhaps more importantly, drones equipped with cameras or telemetry functions will often process personal data, meaning that GDPR obligations may apply in parallel. Drone operators must therefore be aware not only of aviation rules but also of their responsibilities under the main data-protection law in the Union.

As drones become more prevalent, so too does interest in technologies that claim to identify or negate potential threats. Counter-drone systems can generally be divided into two categories: detection technologies and interference technologies. Cyprus treats these categories very differently.

1) **Detection technologies**

   They aim to identify or track drones in a given airspace and may rely on radar, radio-frequency (RF) scanning, acoustic sensors, or optical tools. Passive detection systems—those that merely receive signals without transmitting—are generally permissible to operate.

   However, once a system transmits radio signals, as is the case with active radar, it falls under the scope of the Radio Communications Act of 2002 (Law 146(I)/2002). This legislation requires the prior issuance of a license or authorization from the Department of Electronic Communications (DEC) before any RF-transmitting device can be lawfully operated.

   Operating such equipment without authorization can result in administrative penalties, confiscation of equipment, and, in severe cases, criminal liability. Authorizations are not automatic and are evaluated based on spectrum management, potential interference, and public safety considerations.

2) **Interference technologies**

   Technologies designed to disrupt or “neutralize” drones commonly marketed as jammers, spoofers, or signal-interference devices raise considerably more serious legal issues. These systems work by interrupting a drone’s control link or GPS signal, effectively overriding the pilot’s control. While often presented as a defensive mechanism, they are, in essence, forms of radio interference.

Under Cypriot and EU telecommunications law, **the use of radio-frequency jamming devices is strictly prohibited**, except by specific governmental or authorized military entities acting under controlled conditions. Interference with radio communications carries significant risks, including disruption of aviation signals, emergency services, and other legitimate communications. For this reason, private individuals, companies, hotels, stadiums, security providers, and critical-infrastructure operators are not permitted to deploy jamming systems, regardless of the perceived threat posed by a drone.

There is therefore no general right for private entities to engage in counter-drone "defence." Even when a drone intrudes into private property, endangers safety, or violates privacy, using a jamming device or interfering with its communication signal remains unlawful. The lawful course of action is to rely on passive or authorized detection, record the incident where legally permissible, and report it to the competent authorities.

Only state actors may, under certain circumstances, employ active mitigation tools—and even they are subject to strict operational and legal safeguards.

Looking Forward

As drones continue to evolve, regulators across Europe are exploring whether targeted reforms may be necessary to address security concerns around sensitive sites such as airports, power stations, and government facilities. Until such reforms materialize, however, the legal position in Cyprus remains clear: drone usage is regulated but broadly permitted, whereas counter-drone interference technologies are heavily restricted and, for private actors, effectively prohibited.

In a technological environment where the commercial availability of advanced systems can create false impressions of legality, public awareness of these legal boundaries is essential. Ensuring compliance protects not only the integrity of national infrastructure, but also the safety and rights of the public as drone technologies become an increasingly visible part of everyday life.

ELIAS
NEOCLEOUS
& Co LLC